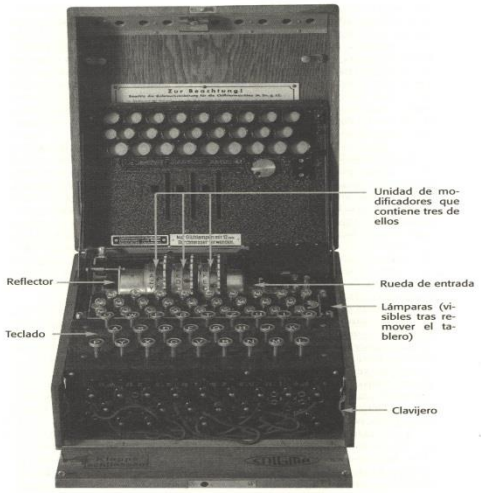
Teoría de las Comunicaciones

Segundo Cuatrimestre del 2014

Departamento de Computación
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Argentina



Seguridad en Redes

Fundamentos

http://www.moonmentum.com/blog/tag/alan-mathison-turing

Agenda

- Marco de Trabajo
- Introducción Criptografía
- Algoritmos de Simétricos y de Clave Publica
- Firma Digital – Integridad
- Autenticación
- Ataques de Red

Marco de Trabajo

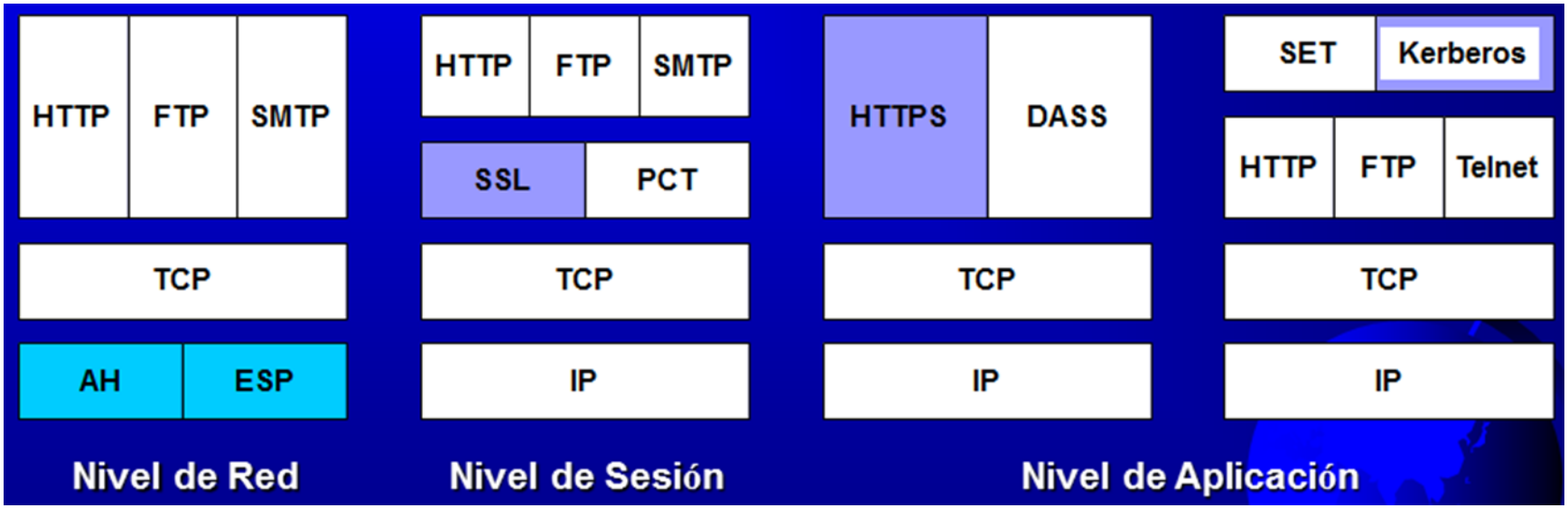
- **Autenticación:** Ninguna parte puede asumir en forma no autorizada la identidad de otra parte.
- **Confidencialidad:** Los mensajes sólo deben ser leídos por las partes especificadas en la comunicación.
- **Integridad :** Los datos enviados no pueden ser modificados durante su transmisión.
- ***No Repudiación*:** Ninguna de las partes puede negar haber participado en una transacción. Por ejemplo: negar el envío de un mensaje.
- **Autorización:** Los servicios brindados sólo pueden accedidos por usuarios autorizados

Seguridad en las Capas

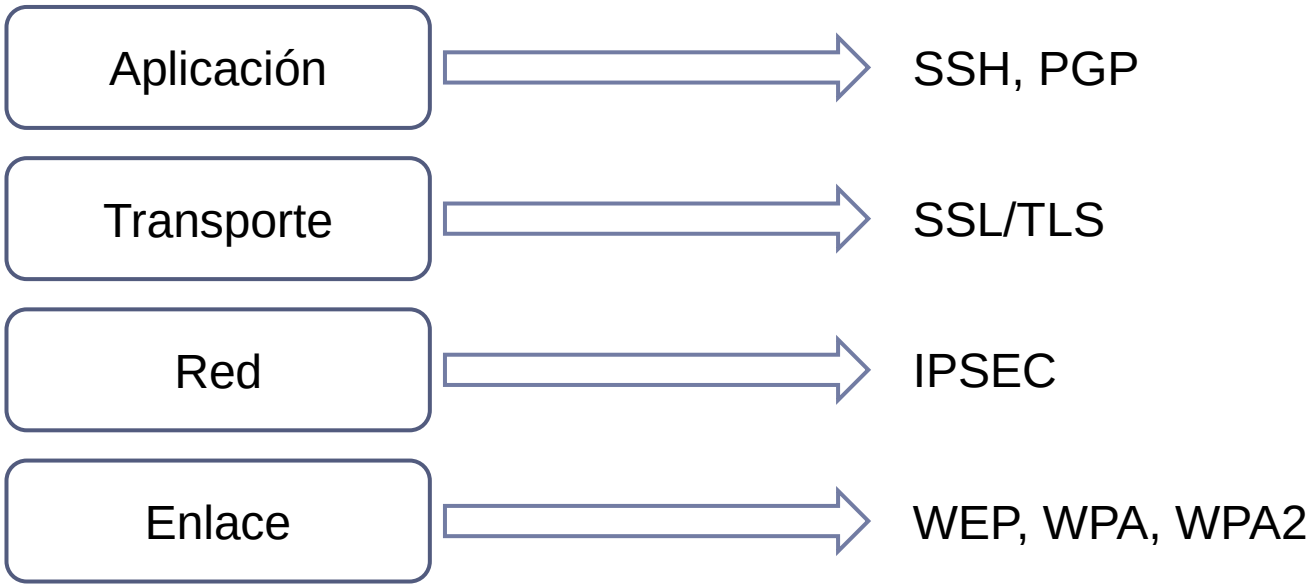
- **Nivel Físico**. El *wiretapping* (intercepción de cables) puede ser evitado encerrando las líneas de transmisión en tubos sellados conteniendo gas argón a alta presión. Cualquier intento de perforar los tubos liberaría el gas reduciendo la presión y disparando una alarma. Esta técnica es utilizada por algunos sistemas militares. Ahora si la comunicación es inalámbrica ?

- **Nivel de Enlace**. Los paquetes en las líneas punto a punto pueden ser codificados en el emisor y decodificados en el receptor en forma transparente a los niveles superiores de red. El problema a esta alternativa se presenta cuando un paquete tiene que atravesar múltiples routers, debido a que dicho paquete debe ser desencriptados en cada router volviéndose vulnerable a ataques dentro del mismo. Por otra parte, esta técnica no permite proteger sesiones en forma selectiva. Sin embargo, la ventaja de la encripción de enlace (*link encryption*) es que la misma puede ser agregada fácilmente.

Seguridad en las Capas



Protocolos: Capas



Introducción a la Criptografía

κρύπτω *krypto*, «oculto», y γράφως *graphos*, «escribir», literalmente «escritura oculta»

Un recorrido rápido ….

- Generacion de numeros al azar
- Hashing
- Claves Simetricas
- Claves Asimetricas
  - Lo "nuevo"……..
- Curvas elipticas
- Criptografia cuantica

Definiciones

- Cifrado
  - Transformación carácter por carácter o bit por bit, sin importar la estructura lingüística del mensaje
- Código
  - reemplaza una palabra con otra palabra o símbolo (ej. Código basado en el "Navajo" usado en el Pacífico II Guerra Mundial)

Métodos Básicos de encriptado

- Cifrado por Sustitución: cada letra o grupo de letras es reemplazado por "idem" . Se Preserva el orden del plaintext .
  - E.j., Cifrado de Cesar ; sustitución monoalfabética (cada letra se mapea con otra; 26!=4x10^26 llaves posibles)
- Transposición: Reorderna las letras pero no las "enmascara"

Principio de Kerckhoff

"Todos los algoritmos deben ser públicos; sólo las claves deben ser secretas"

--- "La Cryptographie Militaire," J. des Sciences Militaires, vol. 9, pp.5-38, Jan. 1883 and pp. 161-191, Feb. 1883.

Longitud de la clave, Factor de Trabajo

- Clave de 2 dígitos decimales → 100 combinaciones.
- 6 dígitos → 1 millón combinaciones
- Claves de 64 bit previene lectura de los mails por hermanos menores … (Tanenbaum)
- Claves de 128 bits uso comercial rutinario
- >256 bits ….

Principios Criptográficos

- Redundancia : *Los mensajes deben contener alguna redundancia*

- Actualización : *Es necesario algún método para frustrar los ataques de repetición*

Principios Criptográficos

- Redundancia : *Los mensajes deben contener alguna redundancia*

- Actualización : *Es necesario algún método para frustrar los ataques de repetición*

Cifrado por sustitución

- Atribuido a Julio César
- Sustitución monoalfabética , claves posibles $26! = 10.4 ** 26$

texto llano:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
texto cifrado:	Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

- Es fácil quebrarlo ? Propiedades estadísticas de los lenguajes naturales …..

Cifrado por Transposición

- La clave del cifrado es una palabra que no contiene letras repetidas. MEGABUCK. El propósito de la clave es numerar las columnas, estando la columna numero 1 bajo la letra clave más cercana al inicio del alfabeto, y así sucesivamente. El texto PLANO se escribe horizontalmente, en filas, las cuales se rellenan para completar la matriz si es necesario. El texto cifrado se lee por columnas, comenzando por la columna cuya letra clave es la más baja.

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Texto llano

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Texto cifrado

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

One-Time Pads ("rellenos de una sola vez")

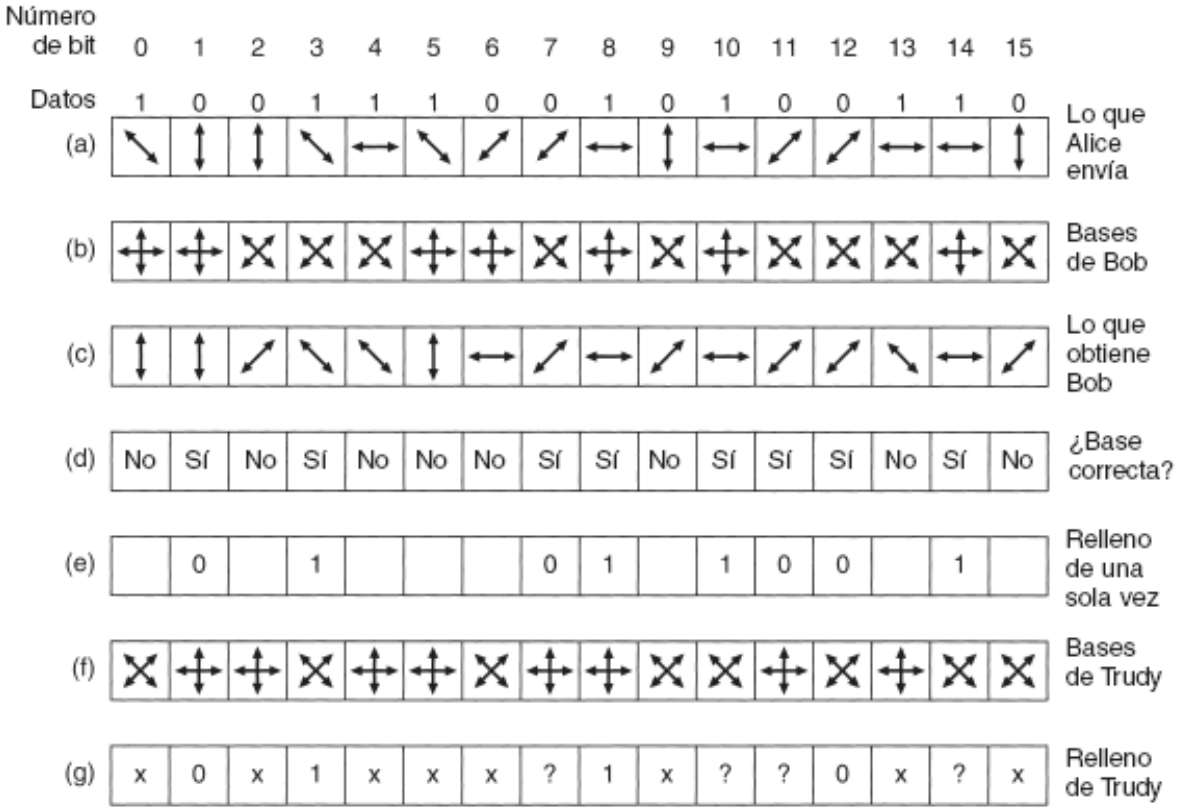
Cifrado Inviolable. Elegir un gran random bit string como clave (= longitud del texto?) Usar Bit XOR como E y D.

"inmune a todos los ataques actuales y futuros sin importar cuánta potencia computacional tenga el intruso " .Teoría de la información: …….

Problema: como distribuir y proteger la clave

Mensaje 1:	1001001 0100000 1101100 1101111 1110110 1100101 0100000 1111001 1101111 1110101 0101110
Relleno 1:	1010010 1001011 1110010 1010101 1010010 1100011 0001011 0101010 1010111 1100110 0101011
Texto cifrado:	0011011 1101011 0011110 0111010 0100100 0000110 0101011 1010011 0111000 0010011 0000101
Relleno 2:	1011110 0000111 1101000 1010011 1010111 0100110 1000111 0111010 1001110 1110110 1110110
Texto llano 2:	1000101 1101100 1110110 1101001 1110011 0100000 1101100 1101001 1110110 1100101 1110011

Criptografía Cuántica

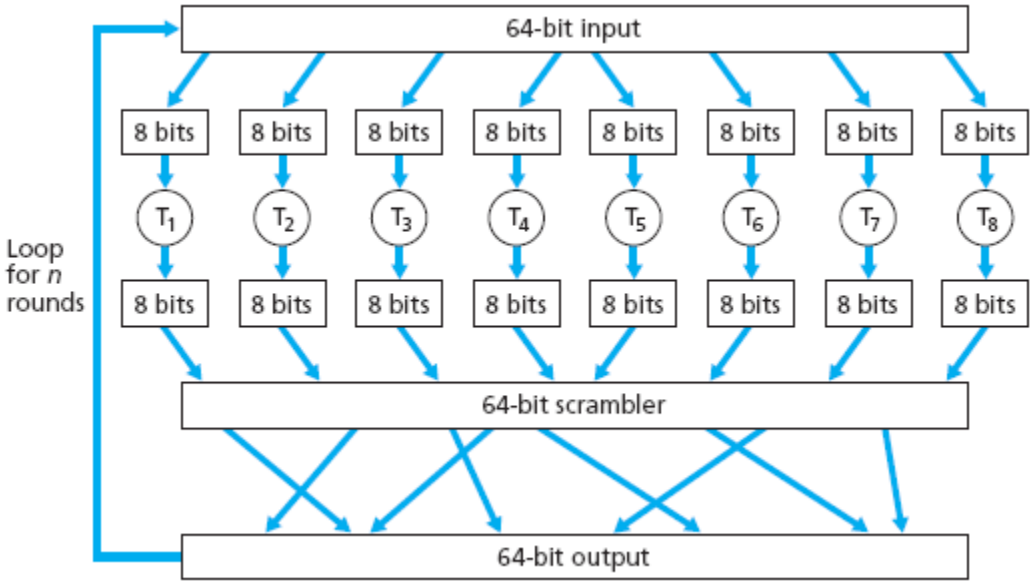


C.H. Bennett and G. Brassard (1984), "Quantum cryptography: public key distribution and coin tossing", Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, IEEE press., pp. 175-179.

Criptografía Cuántica

"Quantum cryptography was proposed first by Stephen Wiesner, then at Columbia University in New York, who, in the early 1970s, introduced the concept of quantum conjugate coding. His seminal paper titled "Conjugate Coding" was rejected by IEEE Information Theory but was eventually published in 1983 in SIGACT News (15:1 pp. 78–88, 1983). In this paper he showed how to store or transmit two messages by encoding them in two "conjugate observables", such as linear and circular polarization of light, so that either, but not both, of which may be received and decoded. He illustrated his idea with a design of unforgeable bank notes. A decade later, building upon this work, Charles H. Bennett, of the IBM Thomas J. Watson Research Center, and Gilles Brassard, of the Université de Montréal, proposed a method for secure communication based on Wiesner's "conjugate observables". In 1990, independently and initially unaware of the earlier work, Artur Ekert, then a Ph.D. student at Wolfson College, University of Oxford, developed a different approach to quantum key distribution based on peculiar quantum correlations known as quantum entanglement."
http://en.wikipedia.org/wiki/Quantum_cryptography

Cifrado Bloque



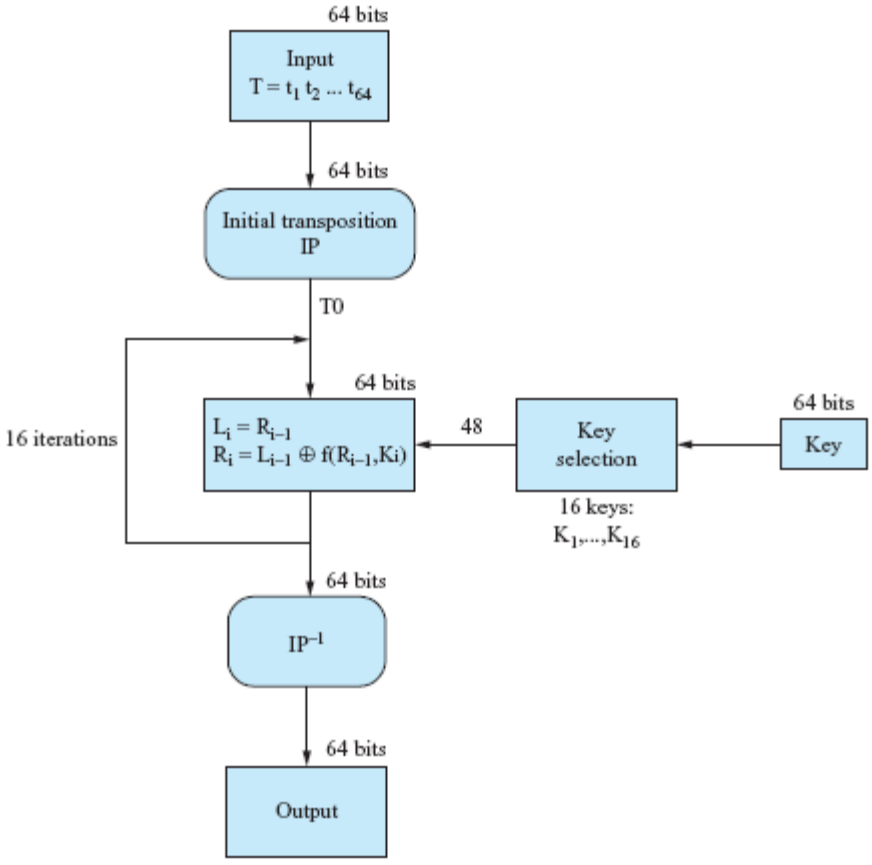
Se toma un bloque de n bits de texto plano como entrada y se transforma utilizando la clave en un bloque de n bits de texto cifrado

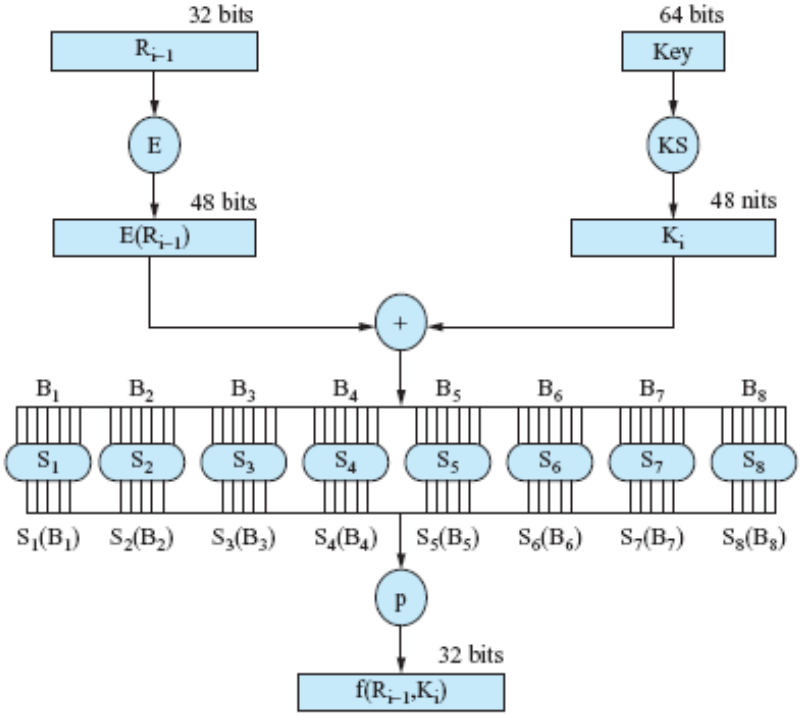
La figura : Computer Networking: Top Down Approach – 6 Edición – pag 680

DES- IBM 1977

- Orientado a bits y no a caracteres.
- Usa tanto transposición como sustitución.
- Trabaja en bloques de a 64 bits.
- Cada bloque ejecuta 16 iteraciones con distintas claves.
- Con el tiempo fue quedando obsoleto el largo de la clave y los ataques por fuerza bruta comenzaron a ser computacionalmente rápidos.
- También se le encontraron vulnerabilidades para algunas claves especificas.
- AES es recomendado hoy en dia. Claves mas largas, es mas rápido y resuelve las vulnerabilidades encontradas en DES.

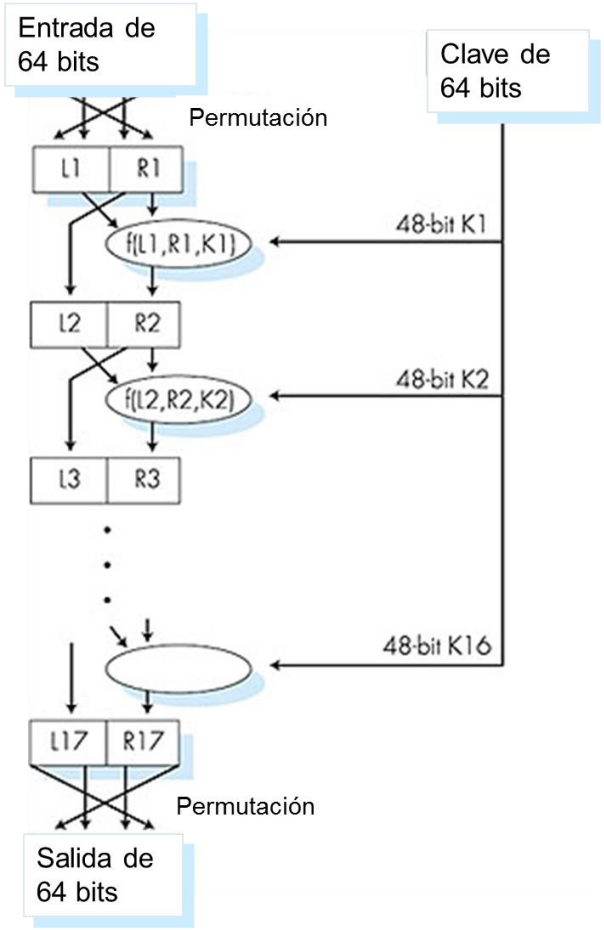
DES (Data Encryption Standard)





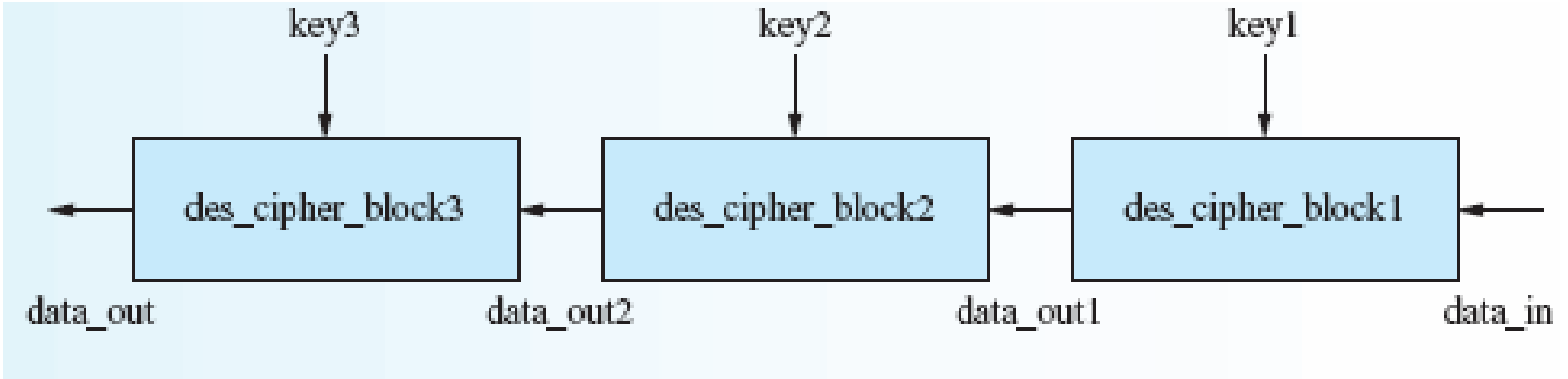
La figura : Computer Networks.: An Open source Approach – 2012 – pags 596-597

DES (Data Encryption Standard)

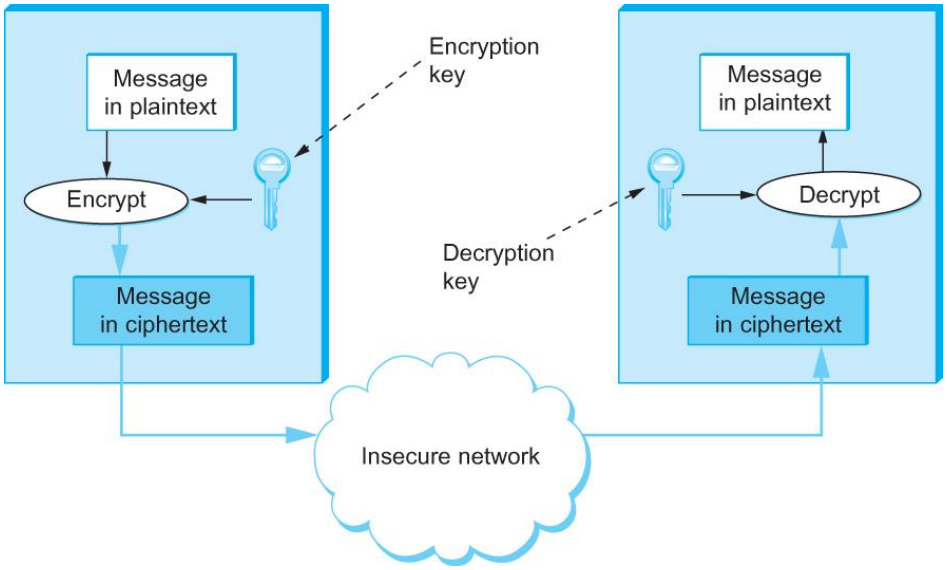


La figura : Redes de Computadores : un enfoque descendente

3 DES (Data Encryption Standard)



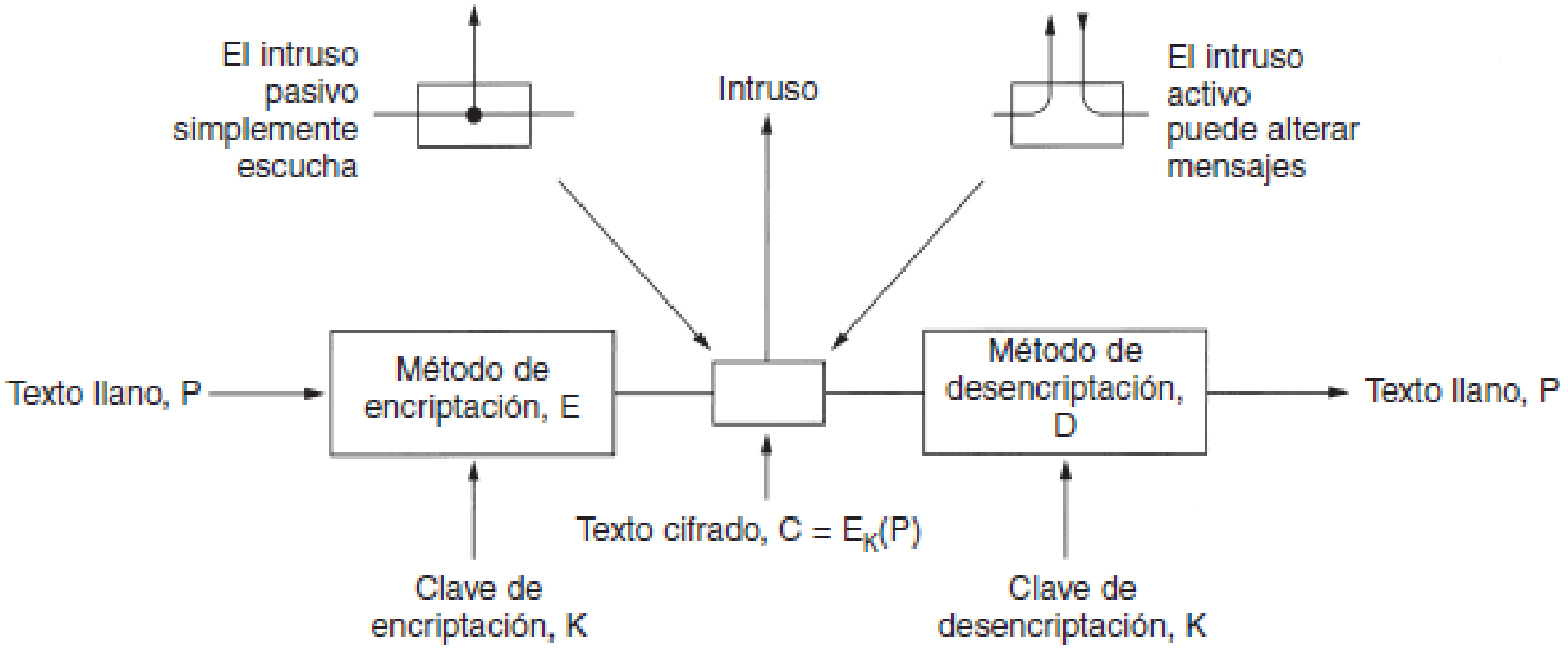
La figura : Computer Networks.: a Open Approach – 4 Edición – pags598



Seguridad en Redes

Algoritmos de clave simétrica – Cifrado por clave privada

Modelo de Encriptación

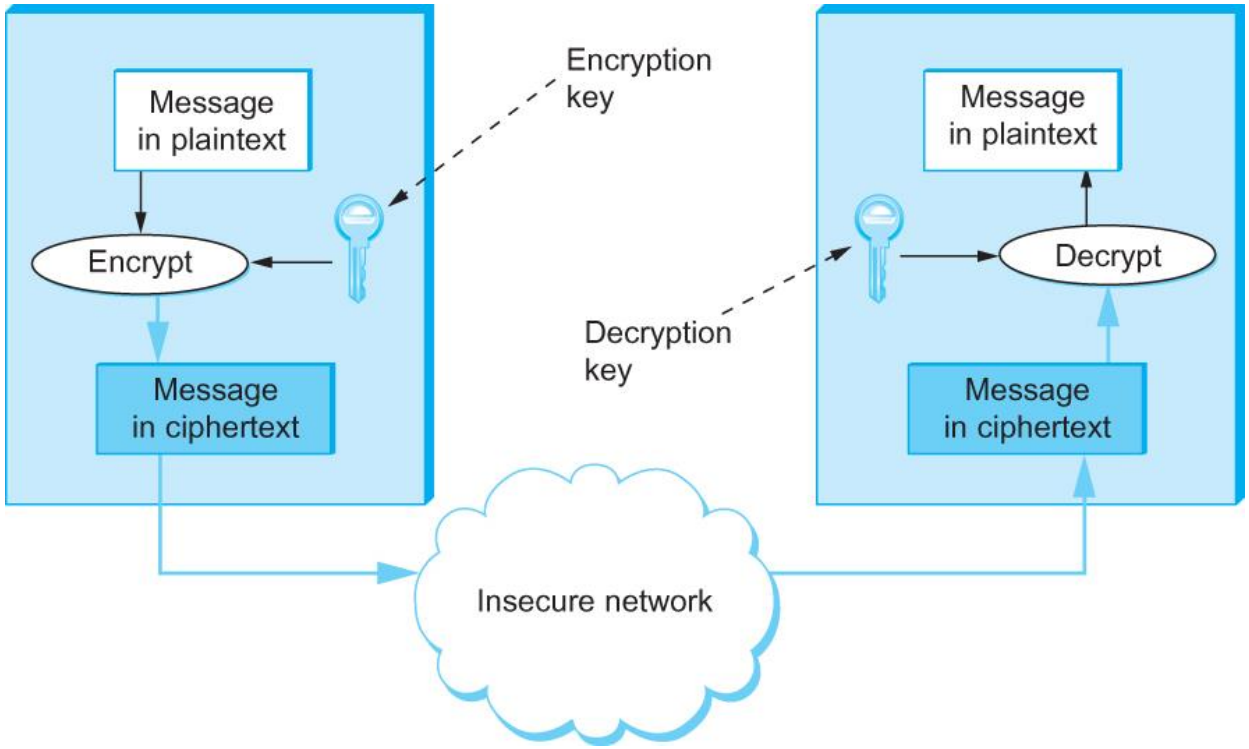


La figura : Tanenbaum – 4 Edición – pag 725

Conceptos

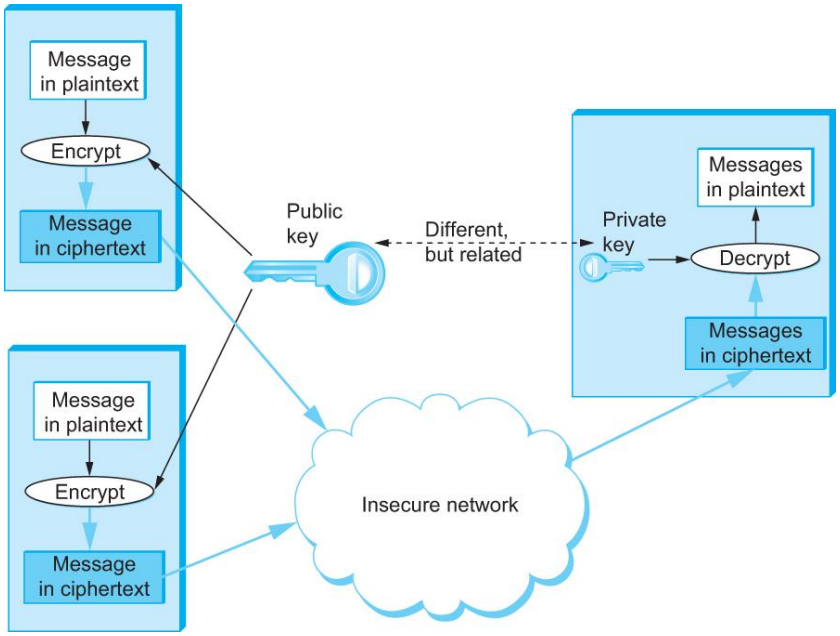
- Los mensajes a ser encriptados se denominan Texto Plano p*laintext* . Son transformados por una función parametrizada por una *clave* .
- La salida del proceso de encripción (cifrado) es conocida como *ciphertext* o texto encriptado y constituye los datos a transmitir.
- Se asume que un *intruso* puede escuchar y copiar el ciphertext completo del canal de comunicación (intruso pasivo).
- La técnica de descifrar mensajes es llamada *criptoanálisis*. La técnica de crear ciphers (*criptografía*) y decifrarlos (*criptoanálisis*) .Ambas forman la *criptología*

Criptografía Simétrica



Notación

- C=EK(P) para representar la encripción del plaintext P usando la clave K con el método de encripción E generando el ciphertext C. En forma similar, P=DK(C) representa la desencripción de C para obtener, nuevamente, el plaintext P. En consecuencia DK(EK(P)) = P.
- Esto sugiere que E y D son funciones matemáticas de dos parámetros, uno de los cuáles representa la clave.



Seguridad en Redes

Algoritmos de clave Asimétrica- Clave Pública

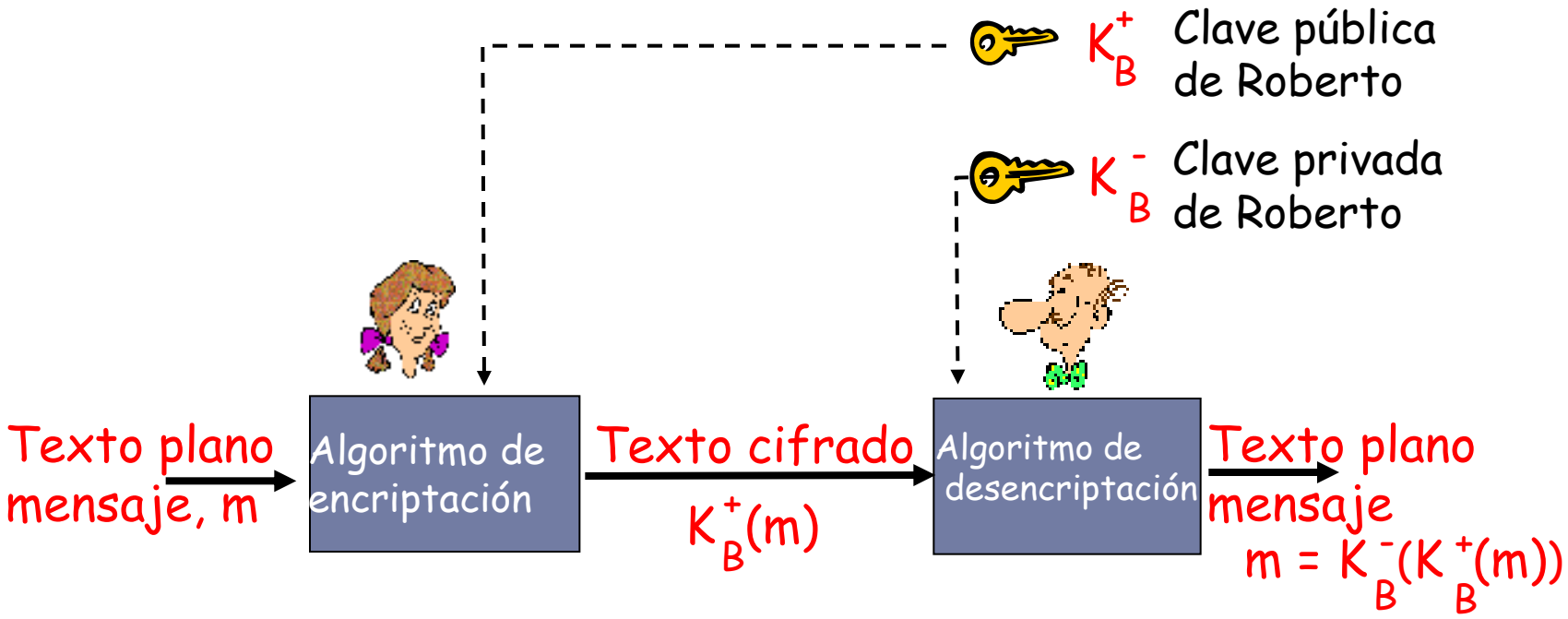
Criptografía de clave Asimétrica

Criptografía de clave simétrica .

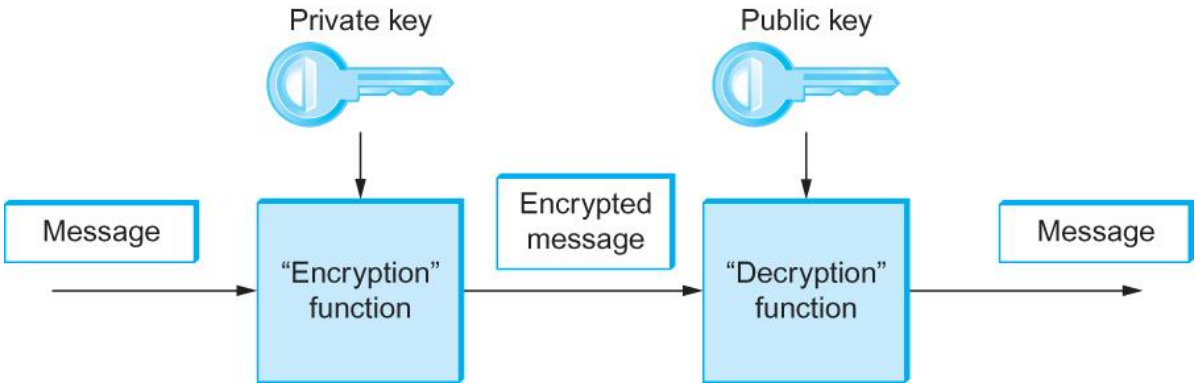
- Requiere emisor, receptor conozca la clave secreta compartida.
- P: ¿Cómo ponerse de acuerdo en la clave, especialmente si nunca se han visto?

- Criptografía de clave pública
- Enfoque radicalmente distinto [Diffie-Hellman 1976, RSA 1978].
- Emisor, receptor no comparten clave secreta.
- Clave de encriptación pública conocida por todos.
- Clave de desencriptación privada, conocida sólo por el receptor

Criptografía de clave pública



Autenticación



Propiedades

- Debe ser fácil cifrar o descifrar dada la clave adecuada
- Debe ser inviable computacionalmente derivar la clave privada a partir de la publica
- Debe ser inviable computacionalmente derivar la clave privada a partir de un texto descifrado (plano)

RSA

- Los conceptos teóricos que sustentan este algoritmo son ciertas propiedades matemáticas respecto a los números primos (factorizar números grandes es costoso), módulos y exponenciación

- Un algoritmo puede encontrar un par de claves, que debido a estas propiedades no son derivables una de la otra, pero tienen la propiedad de ser la inversa

RSA: elegir claves

1. Elegir dos números primos grandes, *p* y *q*. (por ejemplo, 1.024 bits cada uno).

2. Calcular *n* = *pq* y *z* = (*p*-*1*)(*q*-*1*).

3. Elegir *e* (con *e*<*n*) que no tenga factores comunes con *z* (*e* y *z* son primos relativos).

4. Encontrar un número *d* , tal que *ed*-*1* sea divisible de forma exacta entre *z* (en otras palabras, *ed* mod *z* = *1*).

5. La clave *pública* es (*n*,*e*). La clave *privada* es (*n*,*d*).

K_B^+ K_B^-

RSA: encriptación, desencriptación

0. Dados (n,e) y (n,d) calculados anteriormente.

1. Para encriptar patrón de bit , m, calcular:

$c = m^e \bmod n$ (es decir, el resto cuando m^e se divide por n).

2. Para desencriptar el patrón de bit recibidos, c, calcular:

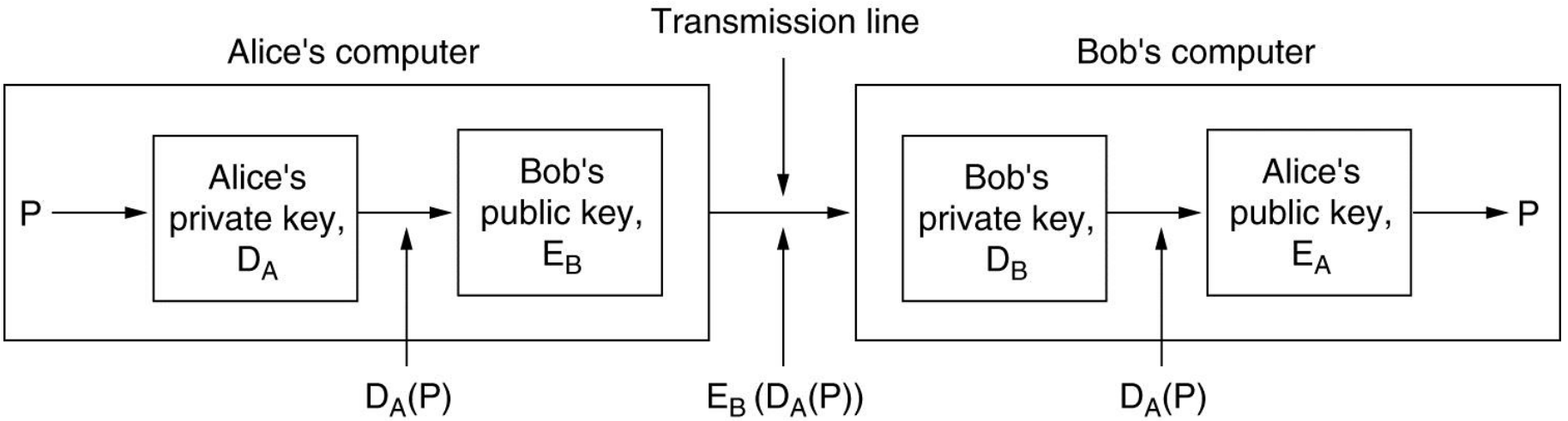
$m = c^d \bmod n$ (es decir, el resto cuando c^d se divide por n).

$$m = \underbrace{(m^e \bmod n)}_{c}^d \bmod n$$

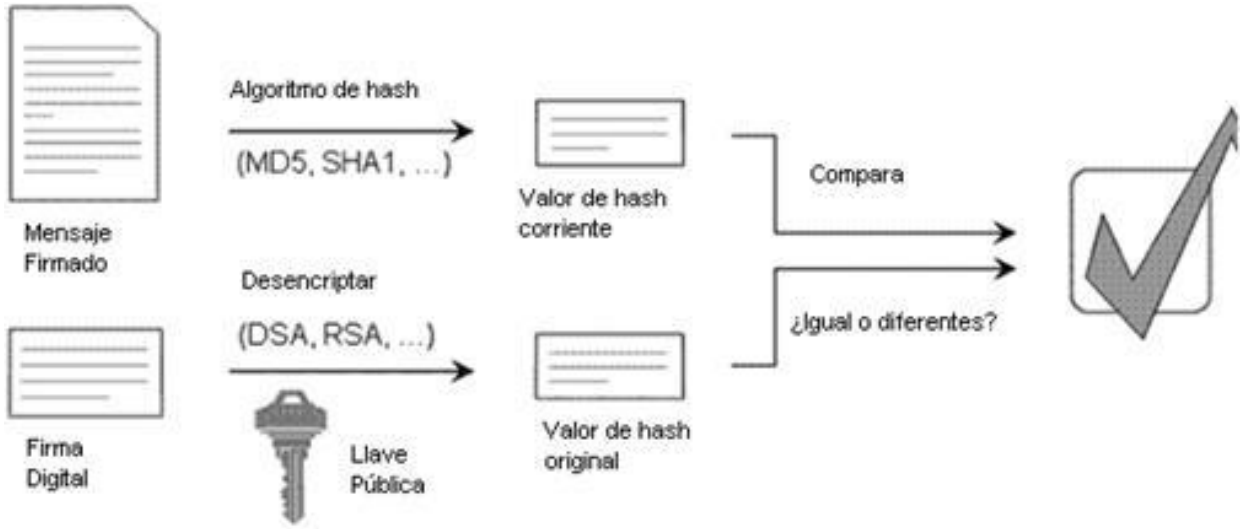
RSA: otra propiedad importante

$$\underbrace{K_B^-(K_B^+(m))}_{\text{Usar primero clave pública, seguida de clave privada}} = m = \underbrace{K_B^+(K_B^-(m))}_{\text{Usar primero clave privada, seguida de clave pública}}$$

Firma Digital con Criptografía Asimétrica



- No repudiación
  - Mediante **cifrado** con la clave Privada
  - Su implementación es eficiente ?



Seguridad en Redes

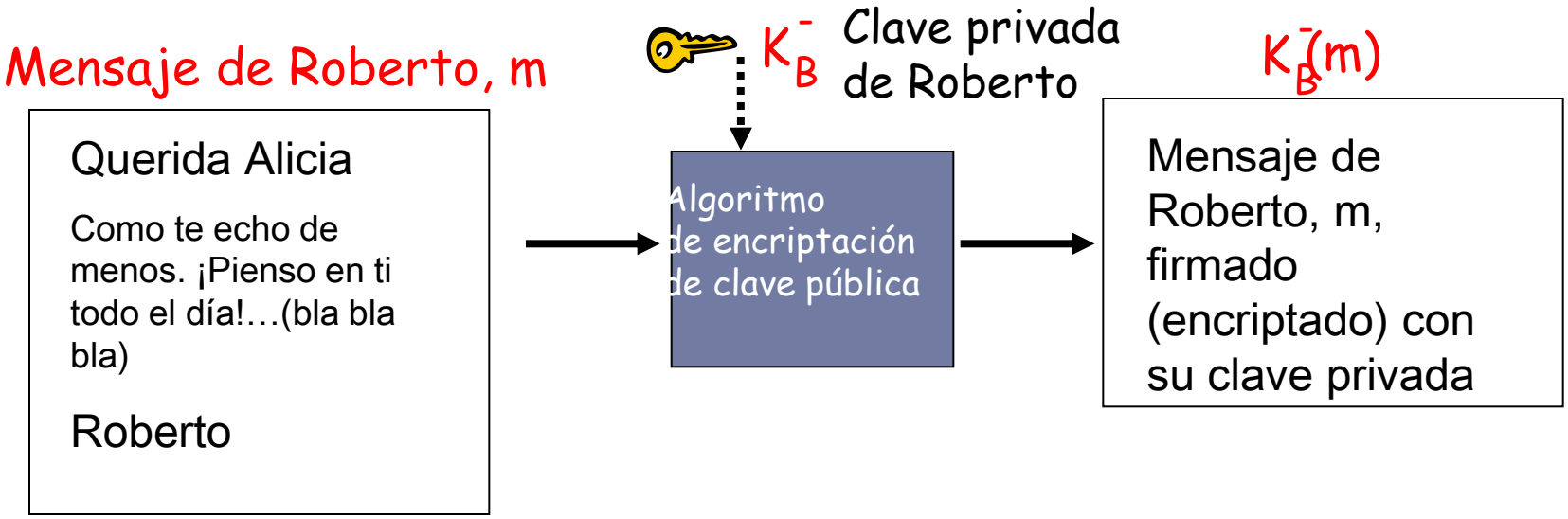
Firma Digital

http://www.cyta.com.ar/biblioteca/bddoc/bdlibros/cifrado_xml/cifrado_xml.htm

Firma Digital

Firma digital simple para mensaje m

- Roberto firma m encriptándolo con su clave privada K_B^-, creando un mensaje "firmado", $K_B^-(m)$



Resumir el mensaje-MD

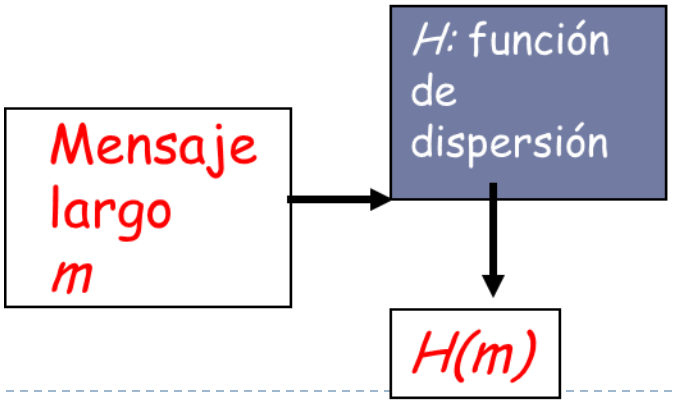
Computacionalmente caro encriptar con clave pública mensajes largos.

Objetivo: longitud fija, fácil de computar

- Aplicar función de dispersión H a *m*, obtener resumen del mensaje de tamaño fijo, *H(m)*.

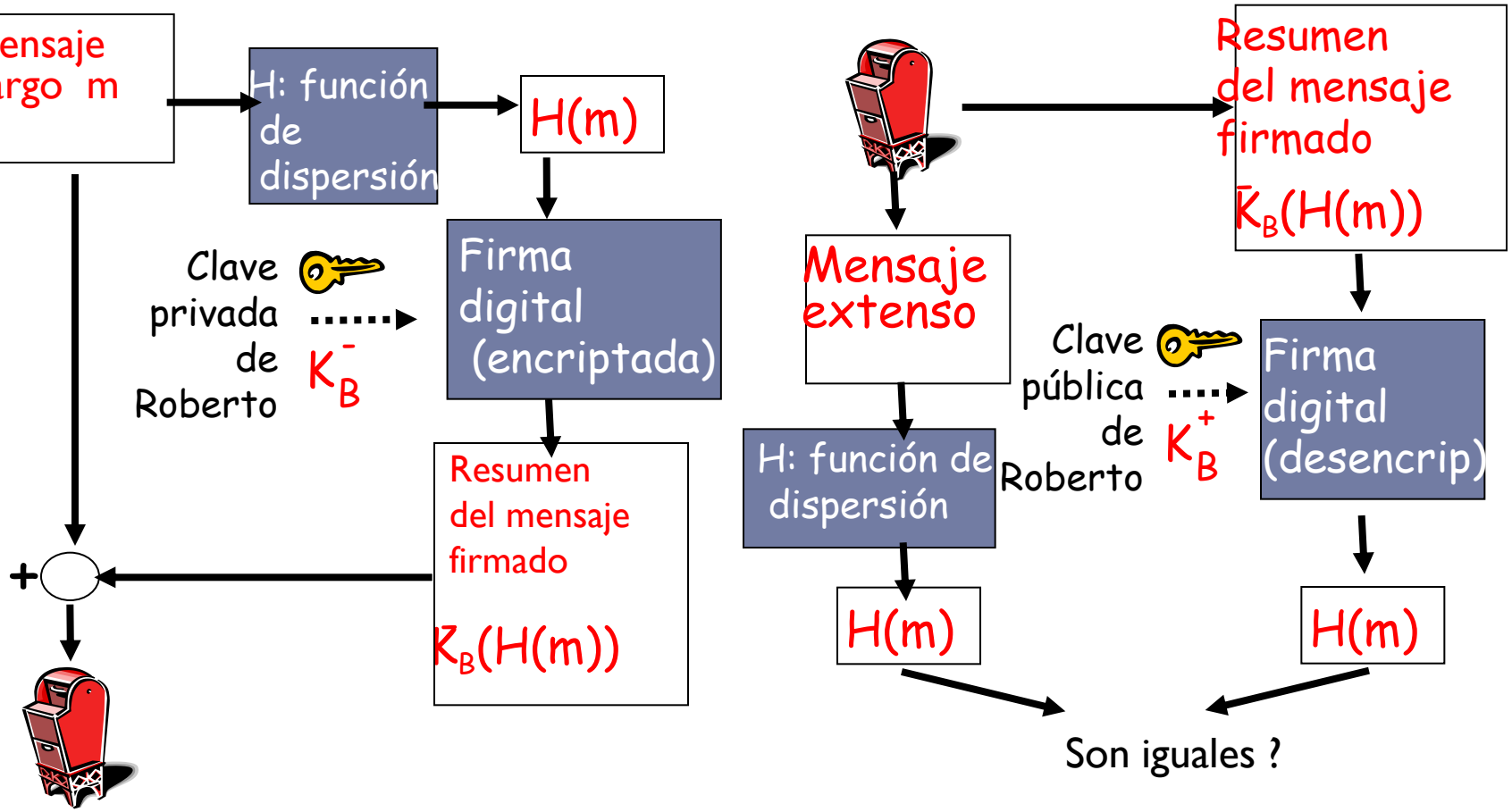
Propiedades de la función de HASH

- Muchos a uno.
- Produce resumen de mensaje de tamaño fijo
- Dado resumen de mensaje x, computacionalmente inviable hallar m para que x = H(m).



Firma Digital : Hash y MD

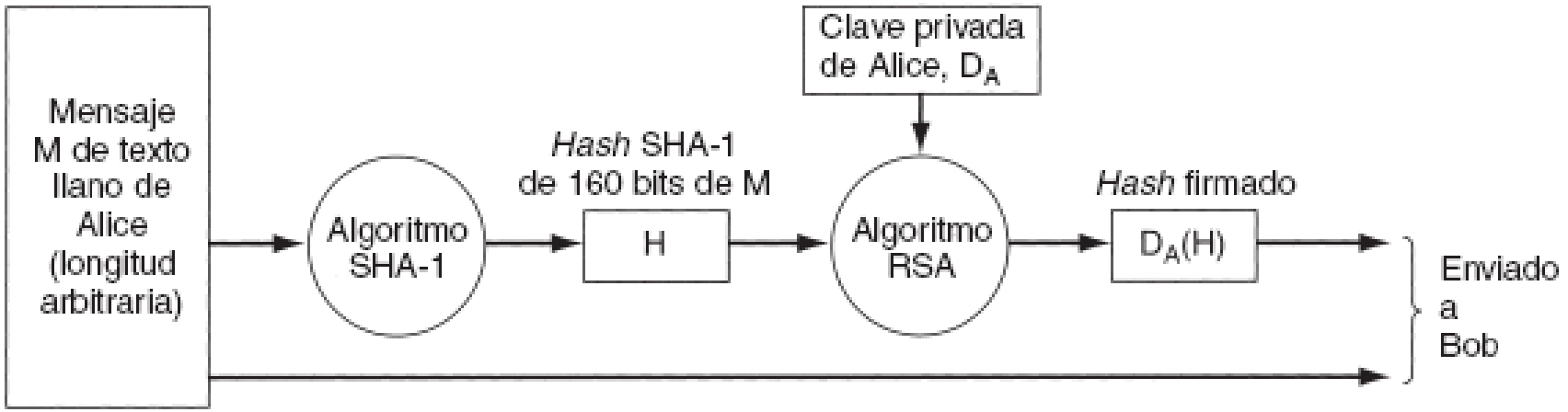
Alicia verifica la firma y la integridad del mensaje firmado digitalmente



Algoritmos para la función HASH

- MD5 función de dispersión ampliamente utilizada (RFC 1321):
  - Calcula un resumen de mensaje de 128 bits en un proceso de cuatro pasos.
  - Cadena x arbitraria 128-bit, parece difícil construir mensaje m cuya dispersión MD5 sea igual a x.
- También se utiliza SHA-1:
  - Estándar de EE.UU. [NIST, FIPS PUB 180-1].
  - Resumen de mensaje de 160 bits.

Firma Digital con RSA y SHA-1



Seguridad en Redes

Integridad

Propiedades

- Consiste en adosarle al mensaje a enviar un checksum que luego puede ser recomputado y constatado para verificar la integridad (similar al checksum de IP).
- Para proveer seguridad se usan funciones de hash con clave o se cifran los hash sin clave

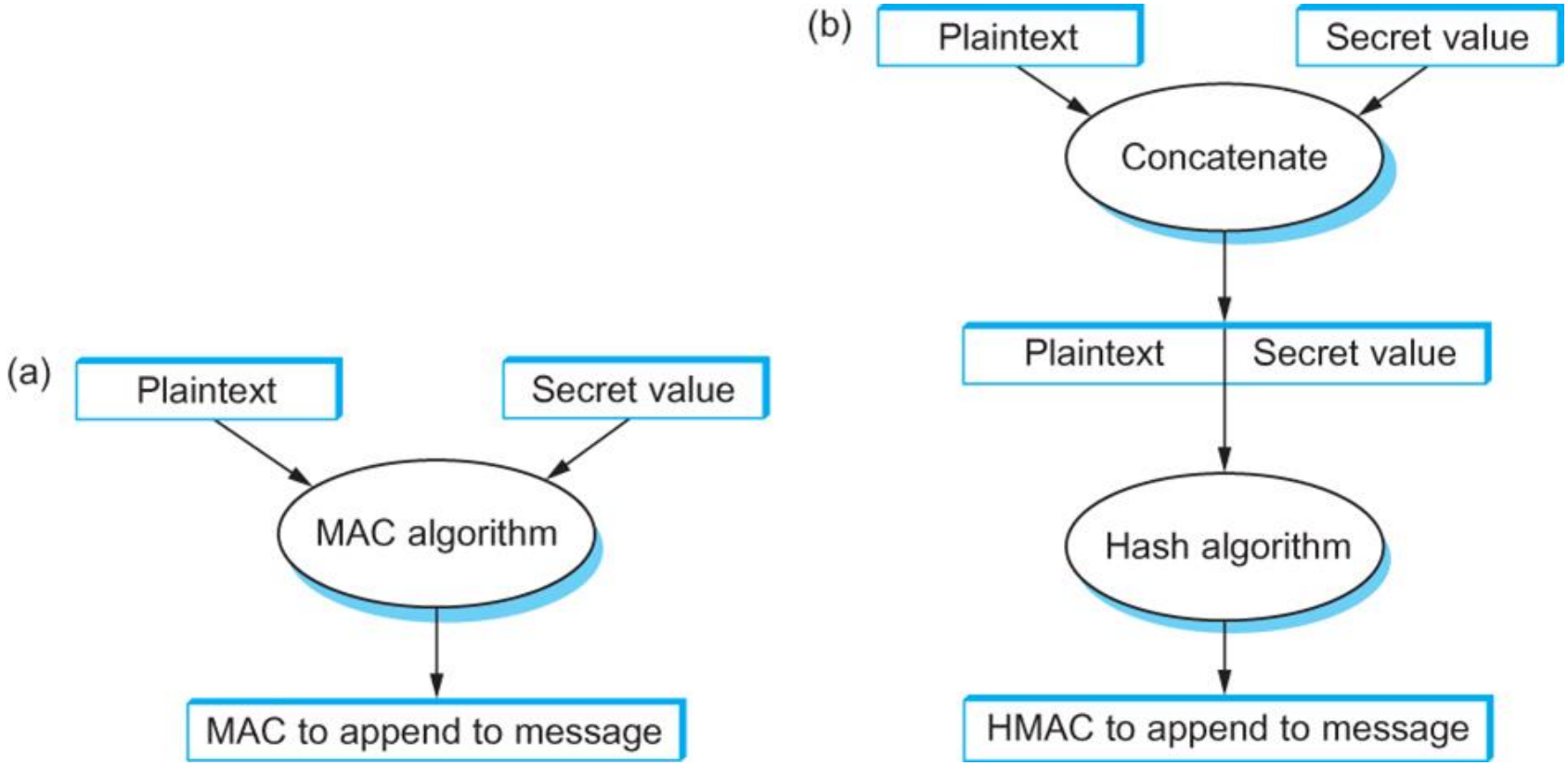
Funciones de hash fuertes (buenas o de ida) $h : A \rightarrow B$

- Dado $x \in A, h(x)$ es fácil de computar.
- $\forall y \in B$ es (comp) inviable encontrar $x \in A$ tq $h(x) = y$.
- es (comp) inviable encontrar $x, \hat{x} \in A$ tq $x <> \hat{x}$ y $h(x) = h(\hat{x})$.

HMAC: hashed message authentication code

- Consiste en hashear el mensaje mezclado con la clave de una manera standard
- Sirve para proveer integridad
- Esta demostrado que la seguridad de HMAC depende de la funcion de hash que se utilice.

MAC - HMAC


(a)
Plaintext
Secret value
MAC algorithm
MAC to append to message
(b)
Plaintext
Secret value
Concatenate
Plaintext
Secret value
Hash algorithm
HMAC to append to message

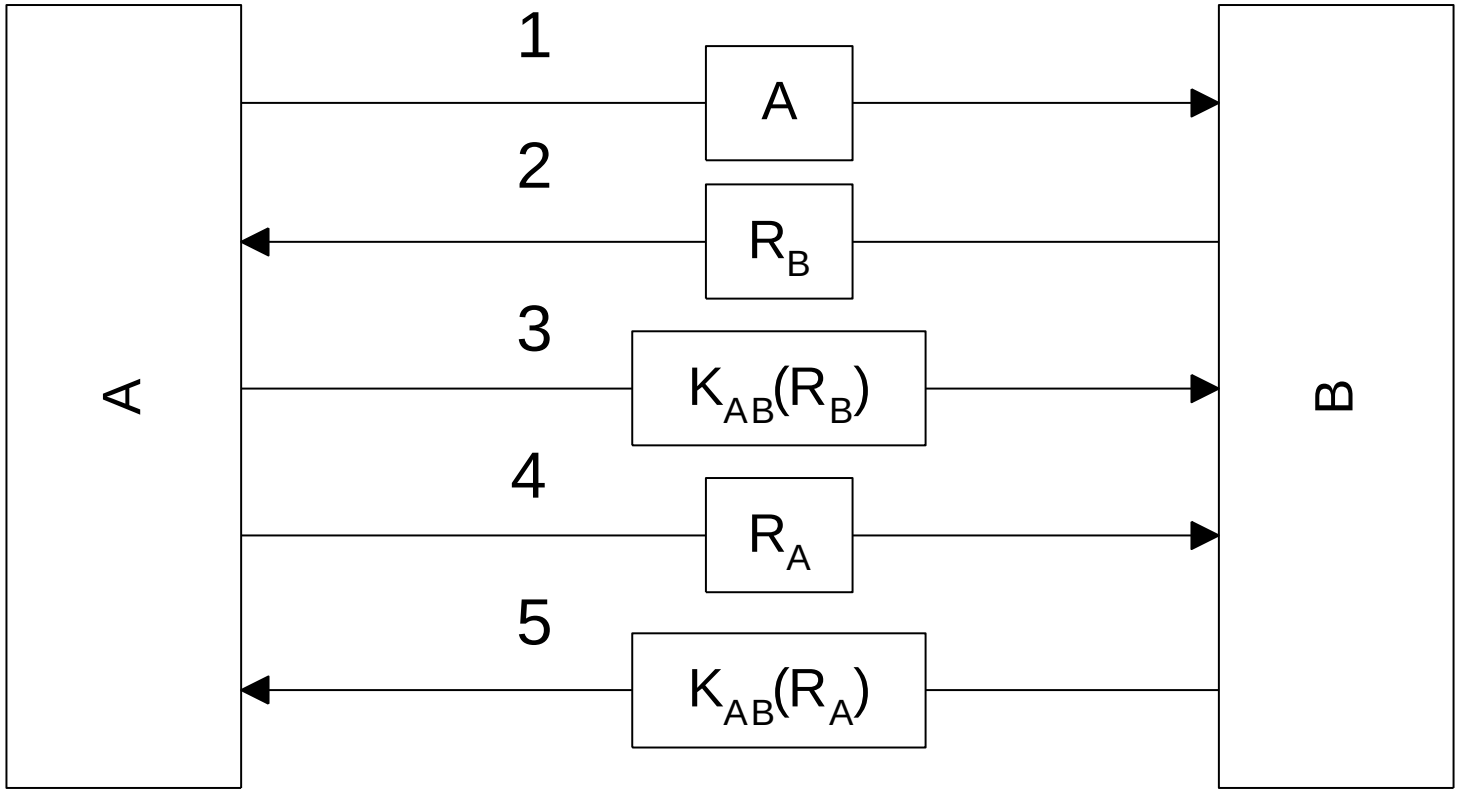
Seguridad en Redes

Autenticación

Autenticación basada en Claves Secretas Compartidas

- 1)A envía su identidad a B.
- 2)dado que todavía B no puede determinar si el mensaje recibido es realmente de A o de un tercero, B elige un *challenge* R_B, (un número random suficientemente grande) y se lo envía a A sin encriptar.
- 3) A encripta el mensaje 2 con la clave que comparte con B, $K_{AB}(R_B)$, y se lo devuelve a B.
- 4)Cuando B recibe este texto cifrado inmediatamente sabe que proviene de A, dado que es el único que conoce la clave K_{AB}.

Autenticación de dos vías



Protocolo "challange-response"

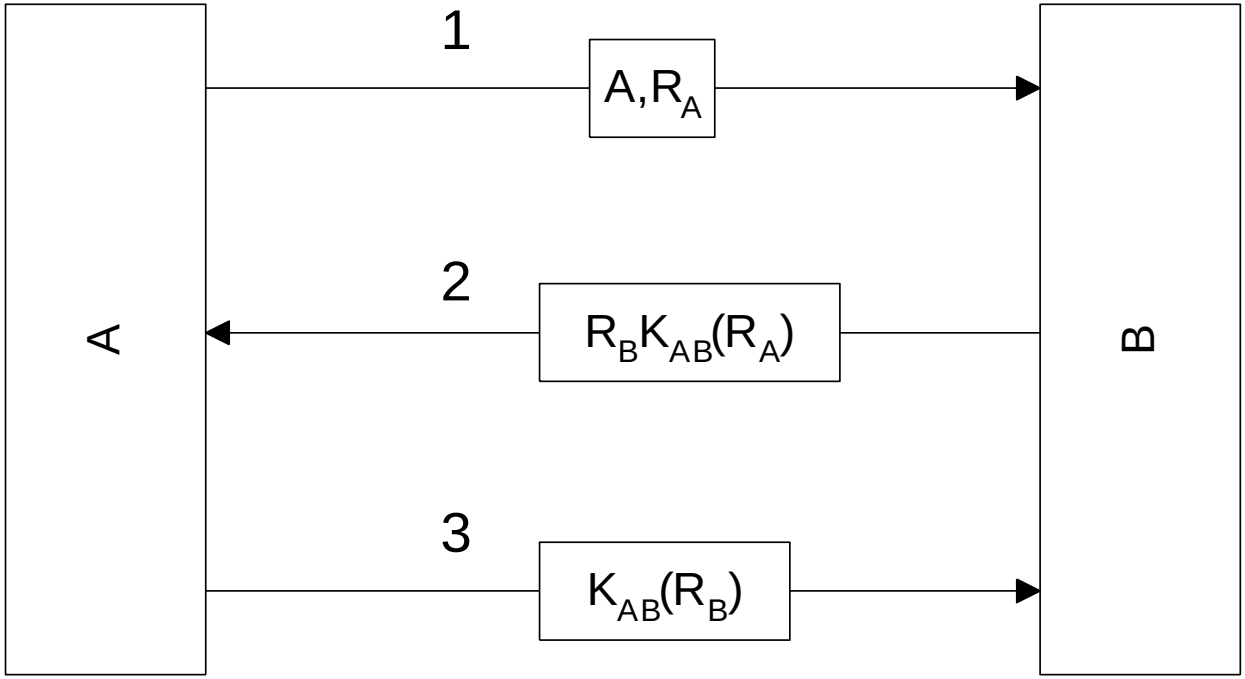
Fuente figura : Tanenbaum – 4 Edición – pag 787

Autenticación basada en Claves Secretas Compartidas

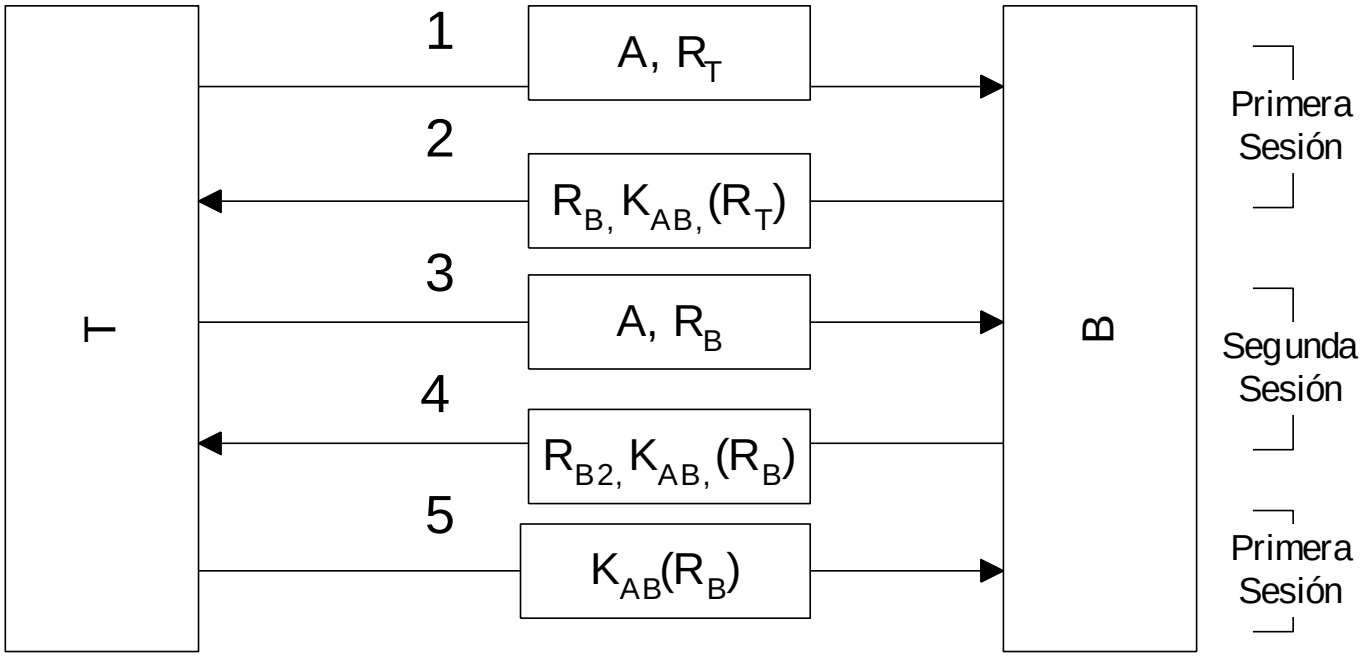
- La elección random y la longitud del *challenge* (p.e: 128 bits) hace realmente improbable que un tercero tome R_B y su respuesta de una sesión previa.
- En este punto B está seguro de la identidad de A, pero este último no posee ninguna garantía a cerca de B. A efectos de verificar la identidad de B, A elige un número al azar, R_A, y se lo envía a B sin encriptar (mensaje 4). Cuando B responde con $K_{AB}(R_A)$, A se asegura de la identidad de B.
- En este momento, si ambos principals desean establecer una clave de sesión, entonces A selecciona un K_S y lo envía a B encriptado con K_{AB}.

Protocolo Autenticación simplificado

Una forma de simplificar la secuencia anterior de envío de mensajes es haciendo que cada principal transmita su identidad y el challenge elegido en el mismo mensaje, sin esperar al envío correspondiente de la otra parte.



Ataque por sesiones



Protocolo "challange-response"

La figura : Tanenbaum – 4 Edición – pag 787

Ataque por sesiones

Si resulta posible establecer sesiones múltiples entre los principals, podría darse la siguiente secuencia:

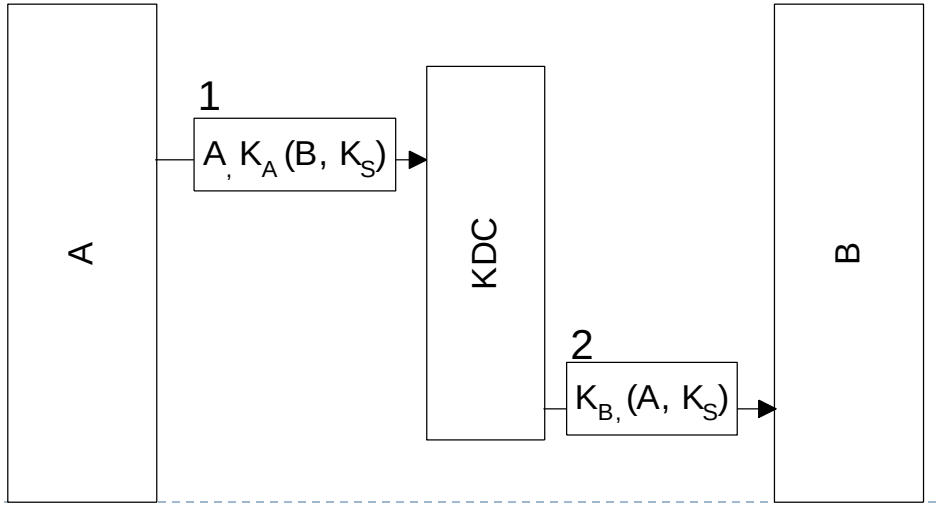
- En el mensaje 1, un tercero T, simula ser A, enviando la identidad de A y R_T.
- En el mensaje 2, B responde como siempre con su challenge R_B, y espera a que A se lo devuelva encriptado.
- En el mensaje 3, dado que T no conoce la clave de encripción, no puede devolver el challenge de B encriptado, entonces inicia una segunda sesión y envía como su challenge R_B.
- Cuando B le devuelve el challenge encriptado $K_{AB}(R_B)$, en el mensaje 4, T utiliza esto como respuesta al mensaje 2 de la primer sesión y aborta la segunda.

Reglas de diseño

- El principal que inicia la transmisión debe probar su identidad en forma previa al principal receptor.
- Ambos principals deben usar claves diferentes para la verificación de identidades, aún cuando esto signifique tener dos claves compartidas K_{AB} y K'_{AB} .
- Deben elegir los challenges de conjuntos diferentes, por ejemplo el que inicia la transmisión del set de números pares y quien contesta a partir de los impares.
- que resista ataques que involucren una segunda sesión paralela, en que la información obtenida se use en una sesión diferente

Distribución de claves confiable (KDC - *Key Distribution Center*)

- A selecciona una clave de sesión K_S y le comunica al KDC su intención de hablar con B. Este mensaje es encriptado utilizando la clave secreta K_A que A comparte solamente con el KDC. El KDC desencripta el mensaje tomando la identidad de B y la clave de sesión y construye un nuevo mensaje conteniendo la identidad de A y la clave de sesión, y lo envía a B encriptado con $K_{B,}$ la clave secreta que B comparte con el KDC. Cuando B desencripta el mensaje, sabe que A se quiere comunicar con él y la clave que desea usar.



Ataques de Red

Spoofing , etc

Ataques de red (1)

- Sniffing
  - Escuchar los datos de la red sin interferir la conexión
  - Para descubrir passwords e información confidencial
  - Protección: encriptación de datos
- Spoofing
  - Hacerse pasar por otro interviniendo una conexión
  - Para acceder a recursos confiados sin privilegios
  - Ataque: "adivinación de nº de secuencia" en TCP
  - Protección: encriptación de protocolo

Ataques de red (2)

- Hijacking
  - Robar conexión después de autenticación con éxito
  - Para acceder a recursos no confiados sin privilegios
  - Protección: encriptación de protocolo
- Ingeniería social
  - Aprovechar la buena voluntad de los usuarios
  - Para tomar privilegios de otros usuarios
  - Ataque: envío de mail como root
  - Protección: autenticación fuerte e información

Ataques de red (3)

- Explotar bugs de software
  - Aprovechar errores de implementación de software
  - Para acceder a recursos sin privilegios
  - Protección: baterías de test y listas CERT
- Confianza transitiva
  - Aprovechar la confianza UNIX entre usuarios ó hosts
  - Para tomar privilegios de otros usuarios ó hosts
  - Ataque: suplantación de dirección IP
  - Protección: autenticación fuerte y filtrado paquetes

Ataques de red (4)

- Ataques dirigidos por datos
  - Ataque diferido originado por datos recibidos
  - Para acceder a recursos sin privilegios
  - Ataque: código javaScript maligno
  - Protección: firma digital e información
- Caballo de Troya
  - Ataque diferido originado por programa recibido
  - Para acceder a recursos sin privilegios
  - Ataque: programa de login falso con base de datos
  - Protección: firma digital e información

Ataques de red (5)

- Denegación de servicio (DoS)
  - Bloquear un determinado conjunto de servicios
  - Para que los usuarios legítimos no lo puedan usar
  - Ataque: "mail bombing" o "ping asesino"
  - Protección: solución ??
- Enrutamiento fuente
  - Modificación de la ruta de vuelta de los paquetes
  - Para acceder a recursos confiados sin privilegios
  - Protección: filtrado de paquetes

Ataques de red (6)

- Adivinación de passwords
  - Prueba sistemática de passwords a un usuario
  - Para que los usuarios no legítimos lo puedan usar
  - Ataque: programa de chequeo de passwords
  - Protección: autenticación fuerte
- Mensajes de control de red
  - Utilizar mensajes ICMP para aprovechar malas implementaciones de la pila TCP/IP
  - Para acceder a paquetes de otra red
  - Ataque: "ICMP redirect" o "Destination unreachable"
  - Protección: filtrado de paquetes